Hide detections with tuning rules

Published: 2022-06-15

Tuning rules enable you to hide detections that match specified criteria.

To avoid creating redundant rules, make sure to first add information about your network environment to the ExtraHop system by specifying tuning parameters.

Learn more about tuning detections.

Add a tuning rule from a detection card

If you encounter a low-value detection, you can create a tuning rule directly from a detection card to hide similar detections in the ExtraHop system.

Before you begin
Users must have full write or higher privileges to tune a detection.

Learn about tuning best practices.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.
3. Click **Actions** from the lower-left corner of the detection card.
4. Click **Tune Detection...**.

   If the detection type is associated with a tuning parameter, you will see an option to suppress the detection. If you still want to create a tuning rule, select the Hide detections like these... option and click Save.
5. Specify the tuning rule criteria and click **Create**.

   The rule is added to the Tuning Rules page. Learn more about managing tuning rules.

Tuning rule criteria

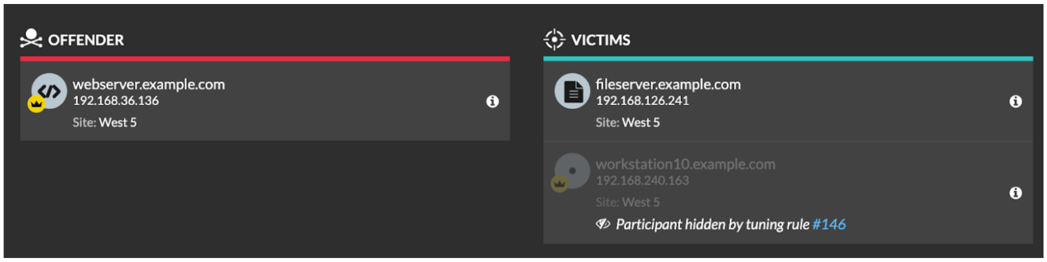
Select from the following criteria to determine which detections are hidden by a tuning rule.

Detection type

You can create a tuning rule that applies to a single detection type, or choose to have the rule apply to all detection types. Rules that encompass all detection types are typically reserved for activity associated with vulnerability scanners.

Participants

Identify participants in a tuning rule by IP address or device name. For detections with multiple offenders you can include a list of IP addresses or CIDR blocks, or reference a device group. You can also create tuning rules that hide a single participant without hiding an entire detection.



OFFENDER

webserver.example.com
192.168.36.136
Site: West 5

VICTIMS

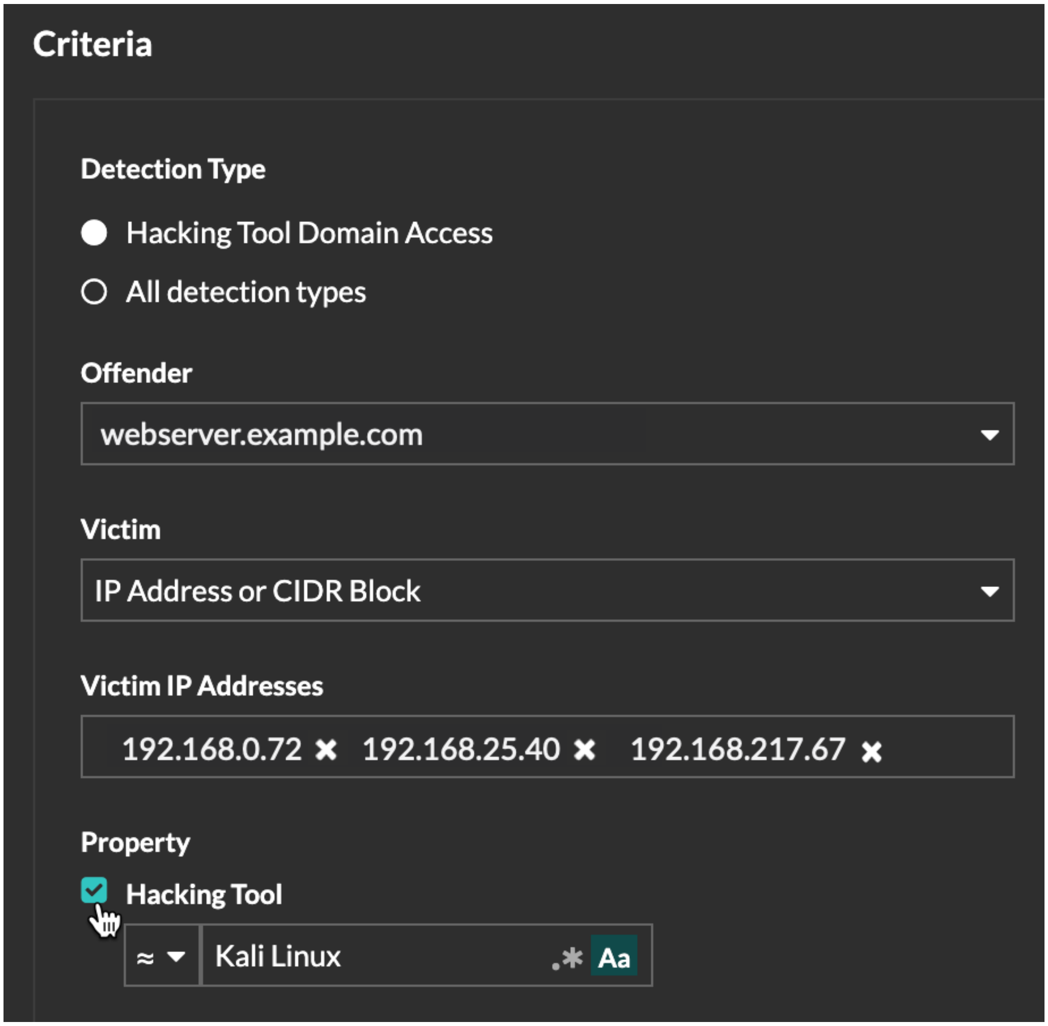
fileserver.example.com
192.168.126.241
Site: West 5

workstation10.example.com
192.168.240.163
Site: West 5
Participant hidden by tuning rule #146

You can opt to hide all offenders or all victims. For example, you can hide the offender in a noisy scan detection regardless of the victim participants.

Detection properties

Create a tuning rule that hides detections by a specific property. For example, you can hide Rare SSH Port detections for a single port number, or Data Exfiltration to S3 Bucket detections for a specific S3 bucket.



Criteria

Detection Type

● Hacking Tool Domain Access

○ All detection types

Offender

webserver.example.com

Victim

IP Address or CIDR Block

Victim IP Addresses

192.168.0.72 ✖ 192.168.25.40 ✖ 192.168.217.67 ✖

Property

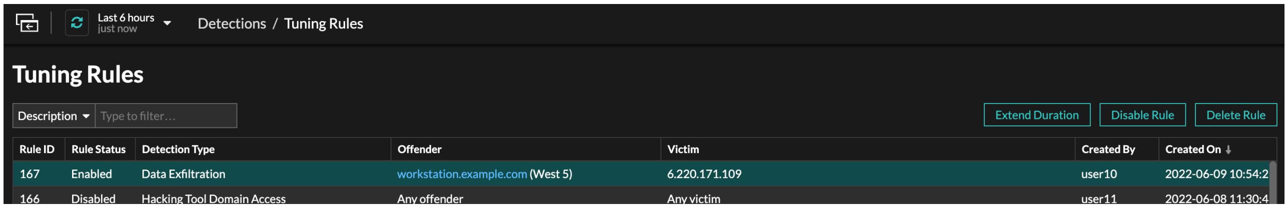
☑ Hacking Tool

≈ Kali Linux

Manage Tuning Rules

You can extend the duration of a rule, re-enable a rule, and disable or delete a rule.

At the top of the page, click the Systems Settings icon ⚙ and select **Tuning Rules**.



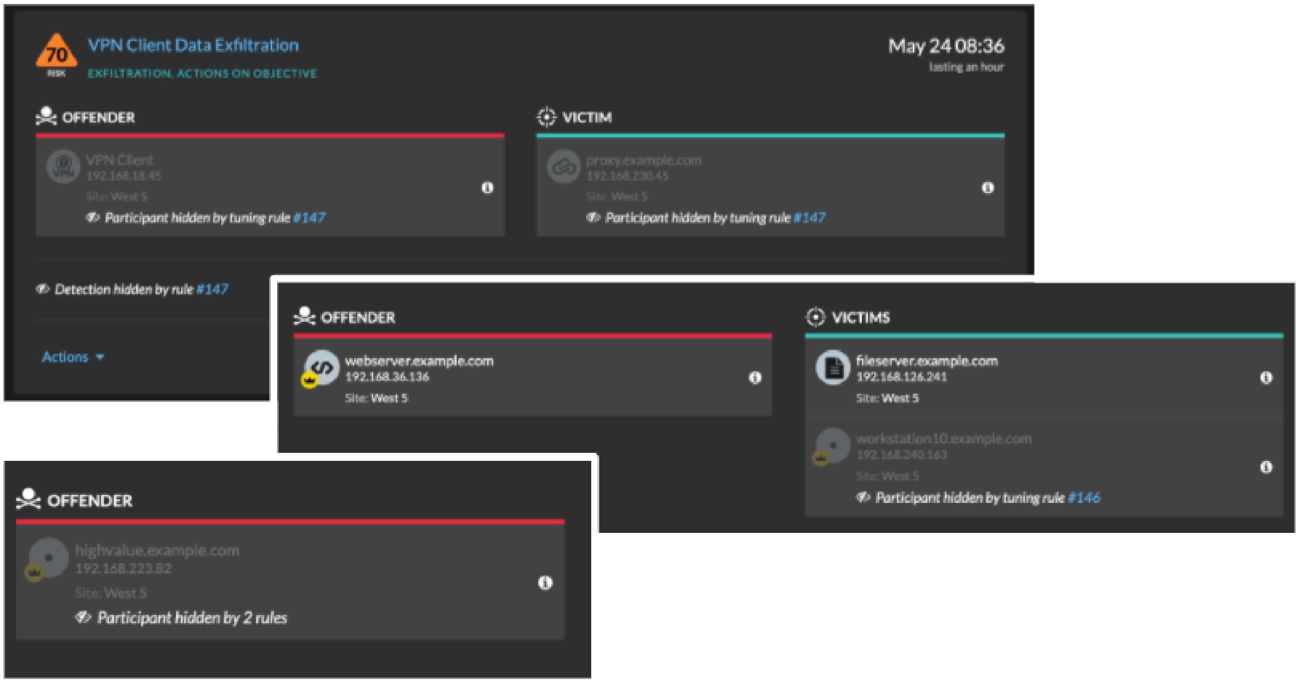
Tuning Rules

Rule ID	Rule Status	Detection Type	Offender	Victim	Created By	Created On ↓
167	Enabled	Data Exfiltration	workstation.example.com (West 5)	6.220.171.109	user10	2022-06-09 10:54:2
166	Disabled	Hacking Tool Domain Access	Any offender	Any victim	user11	2022-06-08 11:30:4

- After you disable or delete a rule, the rule expires immediately and associated triggers and alerts resume.
- After you disable a rule, previously hidden detections remain hidden; ongoing detections appear.

- Deleting a rule displays previously hidden detections.

You can temporarily display hidden detections and participants on the Detections page by selecting the **Show Hidden Detections** checkbox, without disabling the tuning rules. Each hidden detection or participant includes a link to the associated tuning rule, and displays the username of the user that created the rule. If the detection or participant is hidden by multiple rules, the number of rules that apply appears.



70 RISK
VPN Client Data Exfiltration
EXFILTRATION, ACTIONS ON OBJECTIVE
May 24 08:36
lasting an hour

OFFENDER
VPN Client
192.168.18.45
Site: West 5
Participant hidden by tuning rule #147

VICTIM
proxy.example.com
192.168.230.45
Site: West 5
Participant hidden by tuning rule #147

Detection hidden by rule #147

Actions

OFFENDER
webserver.example.com
192.168.36.136
Site: West 5

VICTIMS
fileserver.example.com
192.168.126.241
Site: West 5

workstation10.example.com
192.168.240.163
Site: West 5
Participant hidden by tuning rule #146

OFFENDER
highvalue.example.com
192.168.223.82
Site: West 5
Participant hidden by 2 rules